AMENDMENTS TO THE CLAIMS

1-7 (Canceled).

8. (Currently amended) A quantum-key distributing method for a quantum cryptographic system including a transmission-side communication apparatus that transmits a random number sequence forming a basis of an encryption key in a predetermined quantum state on a quantum communication path and a reception-side communication apparatus that measures a photon on the quantum communication path, the quantum-key distributing method comprising:

transmitting and receiving including

the reception-side communication apparatus maintaining reception data with probability information obtained as a result of measuring a light direction with a measuring device for ~~capable of~~ correctly identifying the light direction; and

the transmission-side communication apparatus maintaining transmission data corresponding to the reception data;

information notifying including the transmission-side communication apparatus notifying, via a public communication path, the reception-side communication apparatus of error correction information generated based on a parity check matrix, of which elements are "0" or "1", and the transmission data, and error detection information generated based on a cyclic code for detecting an error and the transmission data;

transmission-data estimating including the reception-side communication apparatus estimating the transmission data based on a same parity check matrix as that of the transmission-side communication apparatus, the reception data with probability information, the error correction information, and the error detection information; and

encryption-key generating including the transmission-side communication apparatus and the reception-side communication apparatus discarding a part of the transmission data according to an amount of opened information and generating an encryption key using rest of the transmission data.

9. (Previously presented) The quantum-key distributing method according to claim 8, wherein

the transmission-data estimating includes

setting a prior value corresponding to an element "1" in the parity check matrix as initial setting;

executing, row by row, a first process of updating, an external value corresponding to the element "1" in the parity check matrix using a prior value corresponding to another element "1" in an identical row and the probability information according to the error correction information;

executing, column by column, a second process of updating the prior value corresponding to the element "1" in the parity check matrix using an external value after the update corresponding to another element "1" in an identical column;

calculating posterior probability based on the probability information and the prior value after the update and judging a temporary estimated word from the posterior probability; and

detecting, when the temporary estimated word satisfies a predetermined condition established between the temporary estimated word and the parity check matrix, an error for the temporary word using the error detection information, judging, if there is no error, that the

temporary estimated word is original transmission data, and repeatedly executing, when the temporary estimated word does not satisfy the predetermined condition, the first process, the second process, and a process of judging the temporary estimated word using the value after the update until the condition is satisfied.

10. (Previously presented) The quantum-key distributing method according to claim 9, wherein

the transmission-data estimating includes

comparing the error detection information and estimated error detection information generated using the temporary estimated word,

judging, if the error detection information and the estimated error detection information coincide with each other, that there is no error in the temporary estimated word, and

judging, if the error detection information and the estimated error detection information do not coincide with each other, that there is an error in the temporary estimated word.

11. (Currently amended) A communication apparatus that constitutes a quantum cryptographic system in which apparatuses share an encryption key through quantum key distribution, and transmits a random number sequence forming a basis of the encryption key to a quantum communication path in a predetermined quantum state, the communication apparatus comprising:

an information notifying unit that notifies, via a public communication path, the other apparatus of error correction information and error detection information, the error correction

information being generated based on transmission data corresponding to reception data of the other apparatus obtained as a result of measuring a light direction with a measuring device for ~~capable of~~ correctly identifying the light direction and a same parity check matrix as that of the other apparatus, the error detection information being generated based on the transmission data and a cyclic code for detecting an error; and

an encryption-key generating unit that discards a part of the transmission data according to an amount of opened information, and generates an encryption key using rest of the transmission data.

12. (Currently amended) A communication apparatus that constitutes a quantum cryptographic system in which apparatuses share an encryption key through quantum key distribution, and measures a photons, which is a random number sequence forming a basis of the encryption key, on a quantum communication path, the communication apparatus comprising:

a transmission-data estimating unit that estimates original transmission data based on a parity check matrix identical to that of other apparatus that shares the encryption key, reception data with probability information obtained by measuring a light direction with a measuring device for ~~capable of~~ correctly identifying the light direction, and error correction information and error detection information received from other apparatus via a public communication path; and

an encryption-key generating unit that discards a part of the transmission data according to an amount of opened information, and generates an encryption key using rest of the transmission data.

13. (Previously presented) The communication apparatus according to claim 12, wherein

the transmission-data estimating unit performs

setting a prior value corresponding to an element "1" in the parity check matrix as initial setting,

executing, row by row, a first process of updating, an external value corresponding to the element "1" in the parity check matrix using a prior value corresponding to another element "1" in an identical row and the probability information according to the error correction information,

executing, column by column, a second process of updating the prior value corresponding to the element "1" in the parity check matrix using an external value after the update corresponding to another element "1" in an identical column,

calculating posterior probability based on the probability information and the prior value after the update and judging a temporary estimated word from the posterior probability, and

detecting, when the temporary estimated word satisfies a predetermined condition established between the temporary estimated word and the parity check matrix, an error for the temporary word using the error detection information, judging, if there is no error, that the temporary estimated word is original transmission data, and repeatedly executing, when the temporary estimated word does not satisfy the predetermined condition, the first process, the second process, and a process of judging the temporary estimated word using the value after the update until the condition is satisfied.

14. (Previously presented) The communication apparatus according to claim 13, wherein

the transmission-data estimating unit performs

comparing the error detection information and estimated error detection information generated using the temporary estimated word,

judging, if the error detection information and the estimated error detection information coincide with each other, that there is no error in the temporary estimated word, and

judging, if the error detection information and the estimated error detection information do not coincide with each other, that there is an error in the temporary estimated word.